安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 07 月 16 日 (总第 144 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天移动安全发布《微信支付 SDK XXE 高危漏洞预警与应急响应》

近日，微信支付官方 SDK 被曝存在严重的 XXE（XML External Entity Injection，XML 外部实体注入）漏洞。可导致商家服务器被入侵，且攻击者可避开真实支付通道，用虚假的支付通知来购买任意产品。目前，漏洞详细信息以及攻击方式已被公开，影响范围巨大。该漏洞利用成本低，极易被攻击者利用攻击。

漏洞披露后，安天移动安全针对该漏洞及时展开分析，并结合支付行业特点，界定漏洞危害以及对支付行业的影响。第一时间针对支付行业发布微信支付 SDK XXE 高危漏洞预警，并启动了安全应急响应，提出了针对支付行业后台系统的应对措施。

XXE 漏洞是一种容易被忽视但危害巨大的漏洞，它可以利用XML外部实体加载注入，执行不可预控的代码，可导致读取任意文件、执行系统命令、探测内网端口、攻击内网网站等危害。本次被披露的漏洞为服务器漏洞，影响范围为采用 WxPayAPI_JAVA_v3 的微信官方 Java SDK 版本的支付后台系统。

移动支付作为支付行业最主要的业务场景，同时微信支付作为国内主流支付方式之一，绝大部分支付后台均接入微信支付。该漏洞一旦利用会直接导致支付后台数据被窃取，造成重大隐私数据泄露，攻击者还可以基于窃取数据，进行伪造交易等攻击，对支付业务造成极大危害。

针对微信支付 SDK XXE 高危漏洞的威胁态势，目前安天建议从排查和修复两方面入手。支付后台系统运营方就当前接入微信支付 SDK 的支付后台系统进行漏洞专项排查，明确当前支付后台是否存在该漏洞；同时，对于确认存在该漏洞的支付后台，进行相应的威胁处理，对漏洞进行修复。安天可免费提供漏洞检测和修复服务，帮助支付后台系统运营方处置该漏洞威胁。

本次披露的漏洞是一个服务器后台接口漏洞，后台服务作为企业的核心资产，不仅承载着企业核心业务，同时也承载着海量用户的关键数据。一旦服务器存在致命漏洞，受影响的不光是相应企业，同时还有广大用户。因此，如何保护企业核心后台业务安全是企业信息安全的重中之重。企业应当对其核心业务的关键 API 接口进行渗透测试评估，确保核心接口不存在安全隐患。

扫描二维码
阅读报告原文

iOS “USB 限制模式”安全功能被 USB 配件轻松绕过

苹果在 iOS 11.4.1 版本中推出“USB 限制模式”新功能，保护用户设备免遭连接至数据端口的 USB 配件的影响，因此，执法机构和黑客在未经用户许可的情况下很难再破解 iPhone 或 iPad。

如果设备被锁定一小时或更长的时间而端口仍用于为设备充电，那么“USB 限制模式”自动禁用 iPhone 或 iPad 的 Lightning 端口的数据连接功能。换句话说，每当用户锁定 iPhone，后台就激活一小时的倒计时器；如计时完成，则会启用 USB 限制模式以阻止对数据端口的越权访问。

USB 限制模式激活后，如未经用户许可，则无法破解 iPhone 或 iPad。毫无疑问，该功能能够挫败执法部门使用 Cellebrite 和 Grayshift 公司制造的特殊解锁硬件，这些硬件经由 iPhone 的 Lightning 端口尝试猜测密码。

然而，ElcomSoft 公司的研究人员发现了一种简单的方式，可允许任何人重置 USB 受限模式的倒计时器，让新型安全功能形同虚设。

研究人员表示，自上一次解锁手机后，通过直接将 USB 配件连接至解锁 1 小时内的 iOS 设备上，就能重置该设备的 1 小时倒计时器，这个 USB 配件可以是 Apple 的价值 39 美元的 Lightning。

iPhone 配对的 Lightning 配件也能阻止激活“USB 限制模式”。研究人员指出，“换句话说，警官没收 iPhone 后，用户需要立即将 iPhone 连接至兼容的 USB 配件，在一小时后阻止 USB 限制模式。重要的是，只有在 iPhone 仍未进入 USB 限制模式的情况下才起作用。”

ElcomSoft 公司的研究人员还在试验非官方的廉价“USB 适配器的 Lightning”是否也能延伸一小时的时间限制。

这个问题似乎并不严重，而且看似只是苹果方面的错误，希望苹果能很快修复。

同时，用户如果使用的是 iOS 11.4.1，则建议通过“设置→ Face ID & 密码→输入 iPhone 密码”激活该功能，然后向下滚动启用“USB 配件”。

如果用户觉得在倒计时器结束前有必要立即启用 iOS 设备的 USB 限制模式，则按五次电源键即可。

（文章来源：https://thehackernews.com/2018/07/bypass-ios-usb-restricted-mode.html）

每周安全事件

类 型	内 容
中文标题	被盗的 D-link 数字证书可用于签署间谍恶意软件
英文标题	Stolen D-Link Certificate Used to Digitally Sign Spying Malware
作者及单位	Swati Khandelwal
内容概述	安全研究人员最近发现两个恶意软件系列，这些恶意软件使用的有效数字证书属于 D-Link 和另一家名为 Changing Information Technology 的台湾安全公司签署的。其中，Plead 是一个远程控制的后门，旨在窃取机密文件并监视用户。第二个恶意软件为一个类似的密码窃取程序，旨在从谷歌浏览器、IE 浏览器、Microsoft Outlook 和 Mozilla Firefox 收集保存的密码。 研究人员向 D-link 和 Changing Information Technology 通报了该问题，这两家公司分别在 2018 年 7 月 3 日和 7 月 4 日撤销了受损数字证书。
链接地址	https://thehackernews.com/2018/07/digital-certificate-malware.html

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 9 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.ServeSpy.a[prv,spy] 2018-07-09	该应用程序伪装系统应用，激活设备管理器，隐藏图标。对用户语音音频进行录制上传，使用截图截取用户手机屏幕信息上传。上传用户位置信息、手机固件信息、短信、联系人信息、通话记录、浏览器历史记录、手机安装 APP 信息、手机存储文件信息等。造成用户严重的隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.logskit.a[prv,spy] 2018-07-11	该应用程序为一款间谍软件，伪装系统服务，运行后隐藏图标，窃取用户短信、联系人、通话记录、照片、地理位置信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.sanmob.a[exp,rog,sys] 2018-07-11	该应用程序包含恶意代码，运行后联网获取提权工具，root 用户手机，私自下载未知应用，监听用户短信，拦截并解析指定短信，向指定号码发送短信，警惕其私自订阅付费业务。造成用户流量消耗，影响系统安全，建议立即卸载。（威胁等级高）
		Trojan/Android.FakeMSN.a[prv] 2018-07-12	该应用程序伪装 MSN，诱导用户输入账号密码，然后发送到指定邮箱，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Ssnet.a[prv,rmt,exp,spy] 2018-07-12	该应用程序伪装成系统软件，运行时会窃取用户通讯录、通话记录、短信、照片、位置信息，会控制摄像头进行拍照和摄像，还会进行录音，下载未知文件，并且上传用户的隐私信息。造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.Payamak.a[prv,rmt,rog] 2018-07-13	该应用程序伪装 Telegram，运行隐藏图标，拦截短信，接收远程指令弹出虚假下载界面，诱骗用户填写注册码，获取短信内容，点击界面图片会执行拨号、发送付费短信等操作。会造成用户隐私泄露和资费损失，建议立即卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.capushe.b[rmt,exp]	该应用程序隐藏图标，上传手机固件信息，远程控制，接收指令后访问指定网址，打开指定应用，推送广告，下载指定应用，造成用户资费消耗。（威胁等级高）
		Trojan/Android.smssteal.b[prv,exp]	该应用程序运行会窃取用户输入的 Instagram 账号信息，以短信的方式发送至指定号码，造成用户隐私泄露及资费消耗，建议卸载。（威胁等级高）
		G-Ware/Android.bzyUnlock.a[spr,exp]	该应用程序是解锁工具，需要联系作者激活使用，点击会发送短信，还包含勒索程序的下载链接，恶意传播推广勒索软件，建议不要使用。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 远程代码执行漏洞 （CVE-2018-8281）	当软件未能正确处理内存中的对象时，Microsoft Office 软件存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后攻击者可以安装程序，查看、更改或删除数据，或创建具有完全用户权限的新账户。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/Win32.Nurjax	此威胁是一类可以下载恶意代码的木马家族。该家族样本运行后可以劫持浏览器，在用户浏览特定网页时重定向到恶意页面，下载恶意代码并运行。（威胁等级中）
		Trojan[Downloader]/Win32.XorCalc	此威胁是一种具有下载行为的木马类程序。运行后会释放可执行文件；访问远程服务器，下载其它恶意可执行程序；添加注册表信息，并添加计划任务，用来执行恶意程序。（威胁等级中）
		Trojan[Backdoor]/Linux.Mayday	此威胁是一种木马类后门程序，运行在 Linux 平台上。它可以连接远程服务器接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。（威胁等级中）
		Trojan[Downloader]/Win32.Delf	此威胁是一种木马类程序，是使用 Delphi 语言编写具有下载行为的木马类程序，运行后会连接网络并下载其它恶意程序执行。通过以邮件、挂马、捆绑正常软件来进行传播。（威胁等级中）

关于区块链的真相

Jessica Davis / 文　安天技术公益翻译组 / 译

目前，名为“区块链”的分布式账本技术受到很多人的关注。但它真的是你的 IT 项目的解决方案吗?

每年，都会出现一种人人谈论的技术。这种技术会改变一切，将为你的公司带来竞争优势。如果不采用这种技术，你的公司可能会落后。然而，虽然很多人（可能包括公司的首席执行官）都在谈论它，却很少有人真正理解它。在过去的几年中，这些技术包括 3D 打印、自带设备（BYOD）或大数据。而今年，则是区块链。

区块链被认为是许多技术挑战——从创业公司集资到选举投票、出行共享支付、身份证明等等——的解决方案。但是现实情况如何呢?

首先，我们介绍一下区块链的定义。区块链是一种分布式电子账本。每个“区块”包含一条记录。每次添加新区块时，新区块都会包含指向前一个区块的安全链接、时间戳和交易数据。众多区块链接在一起，形成区块链。虽然有些公司提供区块链系统，如 Ethereum、Hyperledger 和 Corda，但是没有任何中央机构控制着区块链。

“区块链可能会对医疗、能源、政府等部门产生重大影响。”麻省理工学院和牛津大学新兴商业讲师，Distilled Analytics 公司首席执行官戴维·夏尔（David Shrier）在接受《信息周刊》（InformationWeek）采访时说。“它不是所有问题的解决方案，但它确实可以应用于很多有趣的领域。”

但是，目前的大多数区块链实现都处于试行阶段，并不是实际的生产系统。夏尔认为，我们正处于一个将改变一切的系统的起步阶段。

“我们可以将目前的区块链比作 1998 年甚至 1994 年的互联网，”夏尔说，“它还处在早期阶段。我们甚至还不理解它的“杀手级应用”（killer app）是什么，但我们已经开始讨论它的应用了 ..... 目前它在实际生产中的部署还很少，但是有很多概念验证。”

夏尔认为，区块链最有趣的用例之一是，它会打破传统风险资本家为创业公司提供资金的方式。根据夏尔的说法，目前的大部分投资集中在加利福尼亚州帕洛阿尔托市的风险投资大街沙丘路（Sand Hill Road），以及其他一些中心。他说，使用区块链作为筹集资金的机制，技术行业可以去中心化，从各个地区获得投资。

夏尔说，另一个有希望的用例是身份验证。他指出，目前世界上有超过 10 亿人没有合法身份，这可能导致他们的信息被利用。

不过，迄今为止，区块链最大的用例还是它一开始设计的用例——作为比特币等加密货币的分布式账本。

定制软件开发公司 3Pillar Global 的首席技术官乔纳森·里弗斯（Jonathan Rivers）在接受《信息周刊》采访时说，在过去的几个月中，每个月都会有客户要求创建区块链解决方案。但实际上，该公司只在大约两年半前为客户构建了一个区块链。

“我们构建那个区块链的原因是，客户想要一个私密的加密货币市场，而这恰恰是区块链的强项。”

里弗斯表示，对于大多数客户的需求来说，区块链威力过大，并不适合。但是，客户们听说过区块链，认为区块链能够解决他们的问题。区块链现在为什么这么热门呢?

“我认为它的主要驱动力是技术无政府主义的概念，或者拥有自由市场的能力。”里弗斯说，“人们希望摆脱中央提供者或控制机构。他们认为，使用分布式账本能够摆脱公司或政府机构的束缚。”

里弗斯指出，区块链不仅有优点——例如安全和去中心化控制，它也有许多缺点。例如，与其他数据库系统相比，它的速度比较慢。

当客户来到 3Pillar Global 公司，要求提供区块链解决方案时，里弗斯通常会打消他们的念头。

“我常跟他们开个玩笑，‘您对消息总线和关系数据库感兴趣不？’”里弗斯说。

里弗斯说，3Pillar Global 着眼于客户希望实现的成果，找到最适合他们的技术。

“客户可能希望建立市场，或存储和分发信息。”他说，“这可以归结为一套更为简单的技术——存储客户记录的数据库、文件存储和正式的身份验证。”

对某些企业来说，区块链的威力可能过大了，但这并不意味着它不能用于未来的用例。在 2017 年 8 月发布的《新兴技术炒作周期报告》中，Gartner 将区块链定位在“期望膨胀期”和“幻觉破灭谷底期”之间，称它离“高峰期”还有 5 到 10 年的时间。而在这 5 到 10 年间，可能会出现很多变化。

原文名称	The Truth About Blockchain
作者简介	Jessica Davis。Jessica Davis 是 Enterprise Apps 的高级编辑。
原文信息	2018 年 7 月 9 日发布于 InformationWeek 原文地址 https://www.informationweek.com/strategic-cio/it-strategy/the-truth-about-blockchain/d/d-id/1332233
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

安天发布《Emotet 恶意木马新变种分析报告》

近期，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时发现 Emotet 恶意木马仍然处于活跃状态，新变种正在不断地被投放。

Emotet 是一类银行木马，当前版本的 Emotet 下载器使用了 Powershell 执行最终命令。其传播途径为电子邮件钓鱼攻击。攻击者使用钓鱼网站，其中包含一个吸引受害者点击的链接，点击后会静默下载恶意代码，该恶意代码通常是一个 Word 文档，它会提示受害者启用宏，一旦开启，VBA 脚本将会在后台执行，下载恶意代码载荷并运行。VBA 代码作为恶意 Office 文档的一部分，只要宏被启用，代码就会在后台执行。作为一种混淆代码的尝试，开发人员添加了大量未被使用的文本，只有整个代码的一部分是可用的，并且它隐藏得很好。初始命令的宏代码是 Sub AutoOpen（），在子过程结束时看到调用了 Application.run 方法，它使用了诸如“DsPBkKtzcIwF”、“ndUzTzJ”等字符，它们分别是生成命令与调用 WScript.Shell 来执行命令的功能。经过多次解密后，可以看到使用了“CMD Comspec /v /c powershell”，调用 Powershell 执行恶意命令。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。

目前，安天追影产品已经实现了对该类恶意代码的检出。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器和静态分析鉴定器将文件判定为木马程序。

概要信息

文件名	707fedfeadbfa4248cfc6711b5a0b98e1684cd37a6e0544e9b7bde4b86096963
文件类型	Document/Microsoft.DOC[:Word 98−2003]
大小	417 KB
MD5	E8E468710C0A4F0906305C435A761902
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Downloader]/MSOffice.Agent.mzr
判定依据	静态分析

运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

常见行为

查找指定内核模块	★★
创建特定窗体	★
获取计算机名称	★
获取驱动器类型	★
请求加载驱动的权限	★
获取系统内存	★★
查找特定窗体	★
获取主机用户名称	★★
获取系统版本	★
设置文件属性为隐藏	★★
隐藏文件	★
独占打开文件	★

文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.doc	e8e468710c0a4f0906305c435a761902	N/A	N/A
~$target.doc	4170cbf55627205688b36dc4fe076bcc	N/A	N/A
GDIPFONTCACHEV1.DAT	c3646290d87aaf9123831d7fd8311319	N/A	N/A
target.doc	403bd882c4b37b3473afa04a5b935be1	N/A	N/A
~WRF0000.tmp	a5c538d59ea156a1a47733aedfbb45f2	N/A	N/A
Normal.dot	347b44ff630ee597656dc805e040a16e	N/A	N/A